S99P1516 0500

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１２月２１日

出 願 番 号
Application Number: 平成１０年特許願第３６２９４２号

出 願 人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

１９９９年１０月２９日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

【書類名】　特許願

【整理番号】　9801061103

【提出日】　平成10年12月21日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 09/32

【発明の名称】　認証システム及び指紋照合装置並びに認証方法

【請求項の数】　12

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　塚村　善弘

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　船橋　武

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【連絡先】　知的財産部　０３－５４４８－２１３７

【手数料の表示】

【予納台帳番号】　005094

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証システム及び指紋照合装置並びに認証方法

【特許請求の範囲】

【請求項１】　保管した情報を操作する際に使用される認証システムにおいて、

使用者の指示を入力する入力手段と、

前記使用者の指示から所定の処理実行を要求する指令コマンドを生成して出力するコマンド出力手段と、

外部機器と通信を行う通信手段と、

を有するホストコンピュータと、

前記ホストコンピュータと通信する通信手段と、

前記通信手段により入力した前記ホストコンピュータからの指令コマンドに応じて所定の処理を行う処理制御手段と、

指紋を検出し指紋データを生成する指紋検出手段と、

前記指紋データ及び前記指紋データに関連付けられた保管情報を記録する保管情報記録手段と、

前記指紋検出手段により検出された指紋データと前記保管情報記録手段に記録された指紋データを照合する指紋照合手段と、

を有する指紋照合装置と、

から成ることを特徴とする認証システム。

【請求項２】　前記保管情報記録手段は、指紋照合結果が一致であった直後の１回のみ、記録された保管情報へのアクセスを許可することを特徴とする請求項１記載の認証システム。

【請求項３】　前記保管情報記録手段は、公開鍵暗号法によって作成される秘密鍵を保管することを特徴とする請求項１記載の認証システム。

【請求項４】　前記指紋照合装置は、さらに暗号鍵の生成及び暗号鍵を用いた暗号化及び復号化を行う暗号処理手段を有することを特徴とする請求項１記載の認証システム。

【請求項５】　前記暗号処理手段は、公開鍵暗号法によって公開鍵及び秘密鍵を作成するとともに前記秘密鍵を用いて暗号文の復号化を行うことを特徴とする請求項４記載の認証システム。

【請求項６】　保管した情報を操作する際に使用される認証システムの指紋照合装置において、

ホストコンピュータと通信する通信手段と、

前記通信手段により入力した前記ホストコンピュータからの指令コマンドに応じて所定の処理を行う処理制御手段と、

指紋を検出し指紋データを生成する指紋検出手段と、

前記指紋データ及び前記指紋データに関連付けられた保管情報を記録する保管情報記録手段と、

前記指紋検出手段により検出された指紋データと前記保管情報記録手段に記録された指紋データを照合する指紋照合手段と、

を有することを特徴とする指紋照合装置。

【請求項７】　前記保管情報記録手段は、指紋照合結果が一致であった直後の１回のみ、記録された保管情報へのアクセスを許可することを特徴とする請求項６記載の指紋照合装置。

【請求項８】　前記指紋照合装置は、さらに暗号鍵の生成及び暗号鍵を用いた暗号化及び復号化を行う暗号処理手段を有することを特徴とする請求項６記載の指紋照合装置。

【請求項９】　保管した情報を操作する際の認証方法において、

ホストコンピュータで、

使用者の指示に応じて指紋照合の要求を使用者に伝えるとともに指紋照合装置に指紋照合指令コマンドを発行する手順と、

指紋照合装置で、

使用者が指紋照合装置に指を乗せた後、指紋を読み取り、

読み取った指紋と登録された指紋の照合を行い、

指紋照合の結果をホストコンピュータに送出する手順と、

ホストコンピュータで、

前記結果が一致の場合に使用者の次の指示を許可し、

前記次の指示の指令コマンドを発行する手順と、

指紋照合装置で、

前記指令コマンドに応じて保管情報にアクセスして所定の処理を行う手順と、

を有することを特徴とする認証方法。

【請求項１０】　前記指令コマンドに応じて保管情報にアクセスして所定の処理を行う手順は、前記照合結果が一致した直後の１回のみ保管情報へのアクセスを許可することを特徴とする請求項９記載の認証方法。

【請求項１１】　前記保管情報は、公開鍵暗号法によって作成される秘密鍵であり、

前記所定の処理を行う手順は、前記秘密鍵を用いて所定の暗号文を復号化する手順であることを特徴とする請求項９記載の認証方法。

【請求項１２】　前記保管情報は、公開鍵暗号法によって作成される秘密鍵であり、

前記所定の処理を行う手順は、公開鍵暗号法により公開鍵と秘密鍵を作成し、

前記秘密鍵を保管する手順であることを特徴とする請求項９記載の認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は本人認証を行う認証システムに関し、特に保管した情報を操作する際に使用される認証システム及び指紋照合装置並びに認証方法に関する。

【０００２】

【従来の技術】

近年、電子マネーを初めとして、電子メールや電子決済等における情報セキュリティの手段として用いられる暗号技術が目覚しい進歩を遂げている。

【０００３】

一般的に電子マネーを使うシステム（例えば、インターネットを使った電子商取引）においては、他者の「なりすまし（他人になりすました偽の取引を行う犯罪）」や、「否認（取引の後に当事者がその事実を否認することによって取引の

債務を逃れようとする犯罪）」を防止することが重要である。このような「なりすまし」を防止するため本人であることを認証する認証や、「否認」を防止するためのデジタル署名技術を応用した証明書発行等に、暗号化技術が用いられている。

【０００４】

この暗号化技術のうちの１つに、公開鍵を用いた公開鍵暗号法がある。公開鍵暗号法とは、一般に公開する公開鍵と当事者が秘密に保持する秘密鍵が作成され、公開鍵で暗号化された文章（注文書や請求書も含む）を、秘密鍵で復号化するという暗号化技術である。公開鍵で暗号化された文章は秘密鍵でのみ復号化可能であり、逆に秘密鍵で暗号化された文章は公開鍵でのみ復号できるという特徴がある。この特徴を利用して、相手認証やデジタル署名が行われる。上記説明のように、公開鍵暗号法における情報セキュリティは、秘密鍵は当事者によって秘密に保持されているということが前提となっている。現時点において、秘密鍵は、コンピュータのハードディスク内や、ＩＣカード等の２次記憶媒体等に秘密鍵を記憶しておき、パスワードにより読み出しを許可する。あるいは、認証機関に保管する。

【０００５】

【発明が解決しようとする課題】

しかし、このような公開鍵暗号法に用いられる秘密鍵を秘密に保持すること、すなわち第三者に知られないように秘密鍵を保存することが難しいという問題がある。現在のところ、公開鍵暗号法により作成された秘密鍵を安全に保存しておくための有力な装置、あるいは技術は見当たらない。

【０００６】

例えば、上記説明のパスワードを付加して保管する方法では、パスワードが破られると、簡単に秘密鍵を取り出されてしまう。また、ＩＣカードに秘密鍵を保存する方法も提案されているが、ＩＣカード内で秘密鍵を暗号化・復号化するためのトリガとしては、パスワードを使わざるを得ない。このため、ホストコンピュータ内部に保管する方法と同様に、パスワードが破られると簡単に秘密鍵を取り出されてしまう。また、認証機関が保存する場合は、非常に機密度の高いシス

テムで管理していることから安全性は高いが、それなりの費用が発生する。

【０００７】

仮に、秘密鍵の保管が万全にできたとして、マクロ的に見ると、コンピュータ内で暗号化・復号化処理を行う際に、秘密鍵が一時的にせよ現れることになる。この時に動作する特殊なプログラムを作成して、秘密鍵を明らかにすることが可能であり、これが行われた場合、その段階で公開鍵暗号法が破綻する。

【０００８】

さらに、上記説明では、秘密に保管する情報を公開鍵暗号法の秘密鍵としたが、他の暗号アルゴリズム、例えばシンメトリック暗号方式（暗号化と復号化を同じ暗号鍵で行う）の暗号鍵の保管や、パスワードの保管や、その他の重要データの保管についても同様であり、安全な保管手段を必要としている。

【０００９】

本発明はこのような点に鑑みてなされたものであり、秘密鍵等の重要なデータを安全に保管する認証システム及び指紋照合装置並びに認証方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】

本発明では上記課題を解決するために、保管した情報を操作する際に使用される認証システムにおいて、使用者の指示を入力する入力手段と、前記使用者の指示から所定の処理実行を要求する指令コマンドを生成して出力するコマンド出力手段と、外部機器と通信を行う通信手段と、を有するホストコンピュータと、前記ホストコンピュータと通信する通信手段と、前記通信手段により入力した前記ホストコンピュータからの指令コマンドに応じて所定の処理を行う処理制御手段と、指紋を検出し指紋データを生成する指紋検出手段と、前記指紋データ及び前記指紋データに関連付けられた保管情報を記録する保管情報記録手段と、前記指紋検出手段により検出された指紋データと前記保管情報記録手段に記録された指紋データを照合する指紋照合手段と、を有する指紋照合装置と、から成ることを特徴とする認証システム、が提供される。

【００１１】

このような構成の認証システムでは、使用者がホストコンピュータの入力手段に指示を入力すると、その指示はコマンド出力手段により指令コマンドとして通信手段を経由して指紋照合装置に送出される。指紋照合装置は、通信手段で指令コマンドを入力し、処理制御手段により入力した指令コマンドに応じた処理を行う。処理が保管情報記録手段に記録された保管情報に関する場合、ホストコンピュータからは最初に指紋照合指令コマンドが送られる。指紋照合装置では、指紋を指紋検出手段で読み取り、指紋照合手段により指紋の照合を行い、一致していた場合に保管情報記録手段へのアクセスを許可するとともに、照合結果を通信手段によってホストコンピュータへ送る。通信手段により照合結果を取得したホストコンピュータは、照合結果が一致していた場合、次の指示を許可する。

【００１２】

また、本発明では、保管した情報を操作する際に使用される認証システムの指紋照合装置において、ホストコンピュータと通信する通信手段と、前記通信手段により入力した前記ホストコンピュータからの指令コマンドに応じて所定の処理を行う処理制御手段と、指紋を検出し指紋データを生成する指紋検出手段と、前記指紋データ及び前記指紋データに関連付けられた保管情報を記録する保管情報記録手段と、前記指紋検出手段により検出された指紋データと前記保管情報記録手段に記録された指紋データを照合する指紋照合手段と、を有することを特徴とする指紋照合装置、が提供される。

【００１３】

このような構成の指紋照合装置は、保管情報記録手段に重要な保管情報とこれをアクセスすることのできる人の指紋データが関連付けて保存されている。保管情報をアクセスする場合には、ホストコンピュータにより指紋照合指令コマンドが発行される。指紋照合装置は、通信手段で指紋照合指令コマンドを入力すると、指紋を指紋検出手段で読み取り、指紋照合手段によって保管情報記録手段に記録された指紋データと前記指紋検出手段で読み取った指紋データを比較して指紋の照合を行い、一致していた場合に保管情報記録手段へのアクセスを許可するとともに、通信手段によりその結果をホストコンピュータへ送る。

【００１４】

また、本発明では、保管した情報を操作する際の認証方法において、ホストコンピュータで、使用者の指示に応じて指紋照合の要求を使用者に伝えるとともに指紋照合装置に指紋照合指令コマンドを発行する手順と、指紋照合装置で、使用者が指紋照合装置に指を乗せた後、指紋を読み取り、読み取った指紋と登録された指紋の照合を行い、指紋照合の結果をホストコンピュータに送出する手順と、ホストコンピュータで、前記結果が一致の場合に使用者の次の指示を許可し、前記次の指示の指令コマンドを発行する手順と、指紋照合装置で、前記指令コマンドに応じて保管情報にアクセスして所定の処理を行う手順と、を有することを特徴とする認証方法、が提供される。

【００１５】

このような手順の認証方法では、ホストコンピュータに指紋照合装置の保管情報にアクセスするような指令が入力された場合、使用者に指紋照合の要求を出すとともに、指紋照合指令コマンドが指紋照合装置に出される。指紋照合装置では、使用者の指紋を読み取り、登録された指紋データと比較して照合を行い、、一致していた場合に保管情報へのアクセスを許可するとともに、結果をホストコンピュータに出力する。ホストコンピュータは、結果が一致であった場合に、次の指令入力を許可する。次の指令が入力されると、それに応じた指令コマンドが発行され、指紋照合装置は所定の処理を行う。

【００１６】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明する。本発明の実施の形態として、本発明の認証システムが最も有効に機能する公開鍵暗号法の暗号鍵の保管について説明する。

【００１７】

ここで、公開鍵暗号法の基本的な原理と使い方について説明する。公開鍵暗号法により、暗号鍵を作成すると、公開鍵と秘密鍵の２つの暗号鍵が作成される。この２つの鍵は、一方の鍵で暗号化した文章は他方の鍵のみ復号化できるという関係にある。このうち、公開鍵は、用いられるシステム（例えば、電子マネーシ

ステム）を使用するすべての人に公開する。秘密鍵に関しては、個人で保管するか、認証機関に保管する。

【００１８】

具体的に電子マネーを使って物を注文する場合について説明する。まず、注文者は、自分の秘密鍵によって暗号化した発注伝票を販売元に送る。販売元では、送られてきた暗号化された注文伝票を、注文者の公開鍵によって復号化する。これが正しく復号化できれば、本当にその人から注文されたことが証明される（この場合、後々本人が注文したことを否認しようとしても、理論的にその本人しか暗号化できない注文書を送ったことから、否認できないことになる）。次に、販売元が注文の品と共に、注文者の公開鍵で暗号化した請求書を注文者に送る。注文者は、その請求書を自分の秘密鍵で復号化し、請求額を支払う。ここで重要なことは、請求書が例えばインターネットのいろいろなポイントを通過している間に、請求金額や振込先等を変更しようと犯罪者が現れても、注文者以外によって復号化できないことから、この様な犯罪は事実上不可能である。このように公開鍵暗号法を使用することで、電子商取引が安全に行われようとしている。

【００１９】

次に、本発明の認証システムについて説明する。図１は、本発明の一実施の形態である認証システムのブロック図である。

本発明に係る認証システムは、本人認証を行う指紋照合装置１００と、指紋照合装置１００への指示等を行うホストコンピュータ２００とが通信ケーブル３００によって接続されている。

【００２０】

指紋照合装置１００は、指紋を光学的に検出し電気信号に変換する指紋検出手段であるＬＥＤ１１１、レンズ鏡筒１１２、ＣＣＤ１１３、及びＡ／Ｄ変換１１４と、読み取った指紋データを照合する指紋照合手段である照合コントローラ１２０と、ＲＡＭ１３０と、保管情報記録手段であるフラッシュメモリ１４０と、処理制御手段であるＣＰＵ１５０、ホストコンピュータ２００との通信手段であるＲＳ２３２Ｃドライバ１６０と、プログラム用ＲＡＭ１７０と、プログラム用フラッシュメモリ１８０と、暗号処理手段である暗号エンジン１９０とから構成

される。

【００２１】

ＬＥＤ１１１、レンズ鏡筒１１２、ＣＣＤ１１３、及びＡ／Ｄ変換１１４は、指が置かれるとＬＥＤ１１１を点灯し、レンズ鏡筒１１２とＣＣＤ１１３により指紋を光学的に読み取る。ＣＣＤ１１３で取り込んだデータをアナログ／デジタル変換（以下、Ａ／Ｄ変換とする）し、デジタイズした指紋データ内の特徴点を指紋データとする。照合コントローラ１２０は、指紋検出手段によって生成された指紋データを、登録されている指紋データと比較して照合を行う。ＲＡＭ１３０は、照合コントローラ１２０の動作時にデータを一時保存するメモリである。

【００２２】

フラッシュメモリ１４０は、指令により指紋検出手段によって生成された指紋データ（以下、テンプレートとする）を記録する保管情報記録手段である。このテンプレートとともに、テンプレートに関連する保管情報、例えば暗号鍵を記録している。このフラッシュメモリ１４０の構成について説明する。図２は、本発明の一実施の形態である認証システムの保管情報記憶部の構成図である。フラッシュメモリ１４０では、指紋１本に対して１つのインデックスが用意されており、本例ではトータル１０００個のインデックスが存在する。このインデックスは２つに分割されており、１つが指紋データの登録エリアであるテンプレートエリアである。もうひとつが、それに付随したアトリビュートエリア、すなわち暗号鍵等の重要な情報を格納しておくエリアである。

【００２３】

図１に戻って説明する。ＣＰＵ１５０は、指紋照合装置１００全体の制御と、ホストコンピュータからの指令コマンドに応じて所定の処理を行う。ＲＳ２３２Ｃドライバ１６０は、ホストコンピュータ２００との通信を行うインタフェースである。プログラム用ＲＡＭ１７０は、プログラム処理実行時のデータを一次保存するメモリであって、ＣＰＵ１５０によりデータの読み書きが行われる。プログラム用フラッシュメモリ１８０は、プログラム処理実行時に使用される。暗号エンジン１９０は、暗号鍵の生成及び暗号鍵を用いた暗号化及び復号化を行う。以下の説明では、暗号エンジン１９０は公開鍵暗号法の処理を行うとする。

【００２４】

ホストコンピュータ２００は、一般的なパーソナルコンピュータ等で、通信ケーブル３００を介して指紋照合装置１００と通信を行う通信手段、指紋照合装置１００への指示コマンドを生成して出力するコマンド出力手段、指紋照合装置１００の状態等を表示する表示手段、及び使用者の指示を入力する入力手段を有する。これらの手段は、一般的なパーソナルコンピュータが有している手段であるので、詳細は省略する。

【００２５】

通信ケーブル３００は、指紋照合装置１００とホストコンピュータ２００を接続する通信ケーブルであり、ここではＲＳ２３２Ｃケーブルである。

このような構成の認証システムの動作及び認証方法について説明する。

【００２６】

使用者が指紋照合装置１００のフラッシュメモリ１４０に保管された保管情報にアクセスする処理を行う場合、ホストコンピュータ２００は、指紋照合を要求するメッセージを表示するとともに、指紋照合装置１００に対して指紋照合指令コマンドを送る。使用者が、指紋照合装置１００の指紋検出手段に指を置くと、指紋検出手段であるＬＥＤ１１１、レンズ鏡筒１１２、ＣＣＤ１１３、及びＡ／Ｄ変換１１４により指紋データが生成される。作成された指紋データは、照合コントローラ１２０により、登録された指紋データと比較されて照合が行われる。照合の結果が一致であった場合、その直後に１回だけフラッシュメモリ１４０に保管された保管情報をアクセスする処理を許可する。また、照合結果はＣＰＵ１５０によってＲＳ２３２Ｃドライバ１６０を経由して通信ケーブル３００で接続したホストコンピュータ２００に送られる。使用者の指示が暗号文の復号化であった場合、指紋照合装置１００へ暗号文が送られる。指紋照合装置１００では、フラッシュメモリ１４０に保管された秘密鍵を取り出し、暗号エンジン１９０により暗号文を復号化し、復号化された平文をホストコンピュータ２００に送る。このように、秘密鍵がホストコンピュータ２００に渡されることはないため、ホストコンピュータ２００から鍵を盗もうとしても不可能であり、非常に安全な認証システムが可能となる。

【００２７】

保管情報へのアクセス処理として、具体的に、保管情報指紋照合装置への指紋データの登録手順、暗号鍵の新規作成と登録手順、及び暗号鍵によって作成されるシンメトリック暗号鍵の復号手順について説明する。以下、ホストコンピュータをＰＣ、指紋照合装置をＦＩＵとする。

【００２８】

第１に、指紋データの登録手順について説明する。ＰＣは、登録コマンドを発行する前に、ＦＩＵ内の登録を指定するインデックスの全てのデータを削除するように、指定のインデックス番号と削除コマンドを発行する。次に、ＰＣから登録コマンドが指定のインデックス番号と共に発行される。ＦＩＵは、上記説明の指紋検出手段により生成した指紋データを、フラッシュメモリ内の指定インデックスに記録する。

【００２９】

第２に、暗号鍵の新規作成と登録手順について説明する。図３は、本発明の一実施の形態である認証システムにおける暗号鍵の新規作成と登録手順のフローチャートである。使用者はＰＣの暗号化アプリケーションにより、暗号鍵の新規作成を指定する（Ｓ０１）。ＰＣからＦＩＵに対して指紋照合コマンドが発行されるとともに、ＰＣディスプレイ上には、「指を指紋照合器（ＦＩＵ:Fingerprint Identification Unit）に載せて下さい」というメッセージが表示される（Ｓ０２）。使用者がＦＩＵに指を載せる（Ｓ０３）と、上記説明の手順で照合が行われ、結果がＰＣに返答される（Ｓ０４）。また、照合がＯＫの場合は、このインデックスに付属しているアトリビュートエリアが開かれる。これは次のコマンドに対してのみ有効であり、その次には再びアトリビュートエリアは閉じられてしまう。ＰＣ側が照合結果を受け取り、それがＯＫの場合（Ｓ０５）、暗号鍵作成コマンドがＦＩＵに対して発行される（Ｓ０６）。ＦＩＵ内では、暗号エンジンにより公開鍵暗号法を用いて秘密鍵と公開鍵が作成され、秘密鍵は上記説明の開かれたアトリビュートエリアに格納される（Ｓ０７）。この後、アトリビュートエリアは閉じる。他方の公開鍵は、ＰＣに返される（Ｓ０７）。ＰＣは、この公開鍵を、暗号システムを使用している相手方に送る。

【００３０】

第３に、暗号鍵によって作成されるシンメトリック暗号鍵の復号手順について説明する。ここでシンメトリック鍵とは、暗号の相手方が特定の文章を暗号化する際に用いる鍵であり、相手方では、シンメトリック鍵によって暗号化された暗号文と、公開鍵によって暗号化されたシンメトリック鍵を送ってくる。暗号システムの過程において、文章をシンメトリック鍵で暗号化するのは、公開鍵（または秘密鍵）での暗号化・復号化よりも計算スピードが速く、時間的に有利だからである。このように、ＦＩＵを用いて公開鍵暗号法により２つの暗号鍵を作成者は、相手方からシンメトリック鍵で暗号化された暗号文と公開鍵によって暗号化されたシンメトリック鍵を受け取る。図４は、本発明の一実施の形態である認証システムにおけるシンメトリック暗号鍵の復号手順のフローチャートである。復号処理時、ＰＣからＦＩＵに対して指紋照合コマンドが発行されるとともに、ＰＣディスプレイ上には、「指を指紋照合器（ＦＩＵ）に載せて下さい」というメッセージが表示される（Ｓ１１）。使用者がＦＩＵに指を載せる（Ｓ１２）と、上記説明の手順で照合が行われ、結果がＰＣに返答される（Ｓ１３）。また、照合がＯＫの場合は、このインデックスに付属しているアトリビュートエリアが開かれる。ＰＣから暗号化されたシンメトリック鍵が復号コマンドとともＦＩＵに送られる（Ｓ１５）。ＦＩＵでは、開かれたアトリビュートエリアから秘密鍵を取り出し、暗号化されたシンメトリック鍵を復号し、これをＰＣに返す（Ｓ１６）。ＰＣでは、この復号されたシンメトリック鍵により暗号文を復号化する。

【００３１】

上記の説明では公開鍵を用いてシンメトリック鍵を暗号化するとしたが、使用者自身の有する秘密鍵でのシンメトリック鍵の暗号化を指紋照合装置内で行うこともできる。

【００３２】

なお、上記の処理機能は、コンピュータによって実現することができる。その場合、認証システム及び指紋照合装置が有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述しておく。そして、このプログラムをコンピュータで実行することにより、上記処理がコンピュータ

で実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場を流通させる場合には、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)やフロッピーディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【００３３】

【発明の効果】

以上説明したように本発明では、例えば秘密鍵等の重要な保管情報をアクセスする場合、最初にホストコンピュータから指紋照合装置へ指紋照合指示コマンドが送られる。指紋照合装置は、指紋の照合を行い、照合結果が一致していた場合のみ本人認証ができたとし、次の指示、すなわち保管情報へのアクセスを許可する。このように、秘密鍵等の重要な保管情報にアクセスする場合には、指紋照合により本人認証を行うので、情報を安全に保管することが可能となる。さらに、例えば、秘密鍵を用いた暗号の復号化処理を指紋照合装置の内部で行えば、秘密鍵は指紋照合装置の外に出ることはない。このため、ハッカー等はホストコンピュータから秘密鍵を盗むことができない。このように、さらに安全な保管が可能となる。また、費用のかかる本人認証機関を利用する必要がない。

【００３４】

また、本発明の指紋照合装置は、ホストコンピュータより指紋照合指示コマンドを入力すると、指紋を指紋検出手段で読み取り、登録された指紋データと比較して指紋の照合を行い、照合結果が一致していた場合にのみ保管情報へのアクセスを許可する。このように、指紋照合装置に保管された秘密鍵等の重要な保管情報にアクセスする場合には、指紋照合により本人認証を行うので、情報を安全に保管することが可能となる。

【００３５】

また、本発明の認証方法は、ホストコンピュータに指紋照合装置の保管情報にアクセスするような指令が入力された場合、使用者に指紋照合の要求を出し、指

紋照合装置で指紋の照合を行う。指紋照合装置は、照合が一致した場合にのみ保管情報へのアクセスを許可する。そして、ホストコンピュータの次の指示に応じて所定の処理を行う。このように、指紋照合装置に保管された秘密鍵等の重要な保管情報にアクセスする場合には、指紋照合により本人認証できた場合のみアクセスを許可するので、情報を安全に保管することが可能となる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態である認証システムのブロック図である。

【図２】

本発明の一実施の形態である認証システムの保管情報記憶部の構成図である。

【図３】

本発明の一実施の形態である認証システムにおける暗号鍵の新規作成と登録手順のフローチャートである。

【図４】

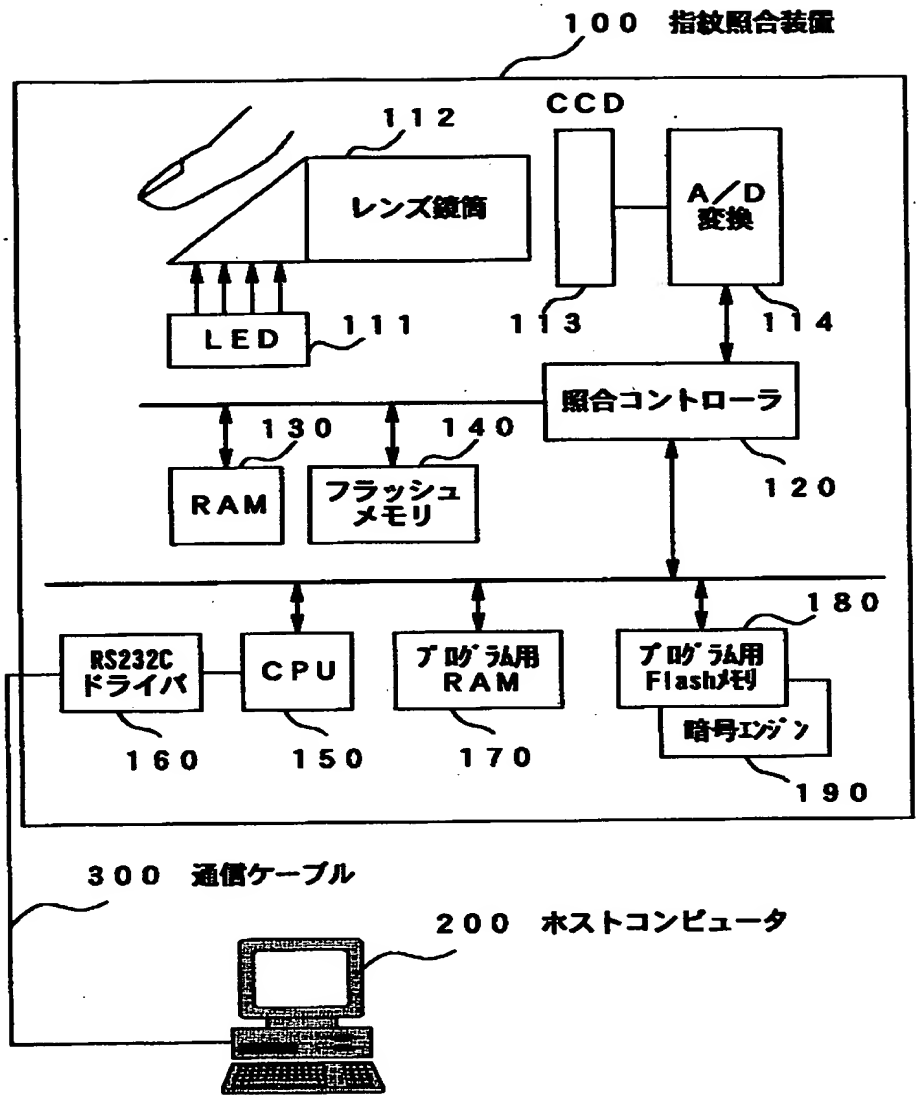
本発明の一実施の形態である認証システムにおけるシンメトリック暗号鍵の復号手順のフローチャートである。

【符号の説明】

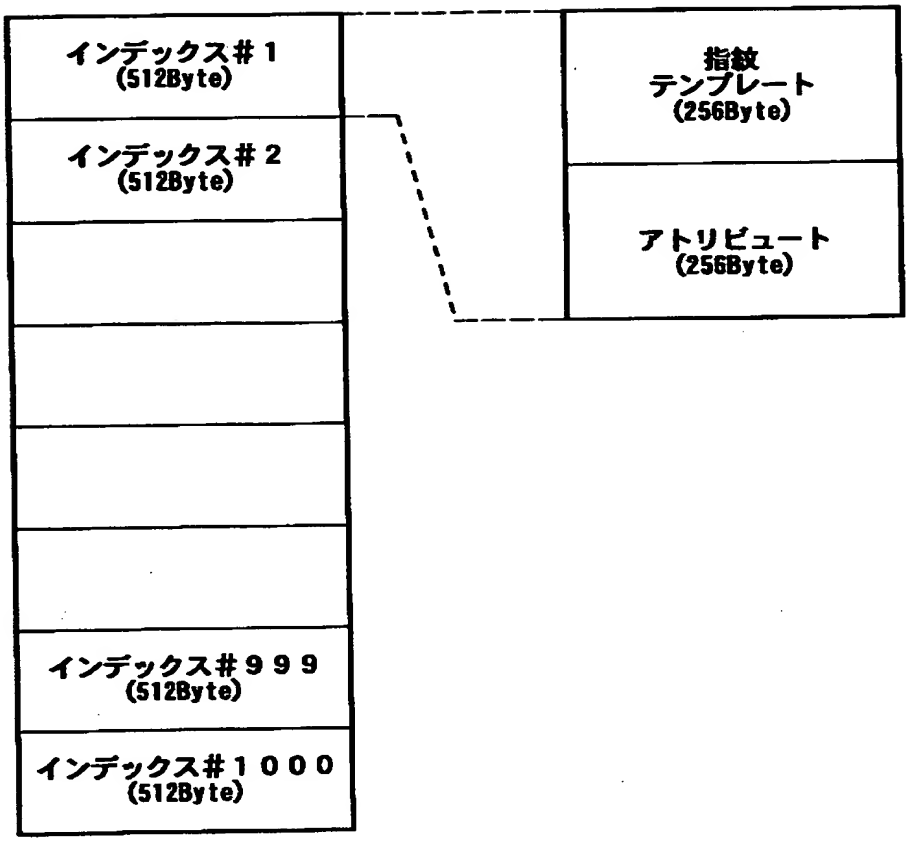
１００…指紋照合装置、１１１…ＬＥＤ、１１２…レンズ鏡筒、１１３…ＣＣＤ、１１４…Ａ／Ｄ変換、１２０…照合コントローラ、１３０…ＲＡＭ、１４０…フラッシュメモリ、１５０…ＣＰＵ、１６０…ＲＳ２３２Ｃドライバ、１７０…プログラム用ＲＡＭ、１８０…プログラム用フラッシュメモリ、１９０…暗号エンジン、２００…ホストコンピュータ、３００…通信ケーブル

【書類名】　　図面

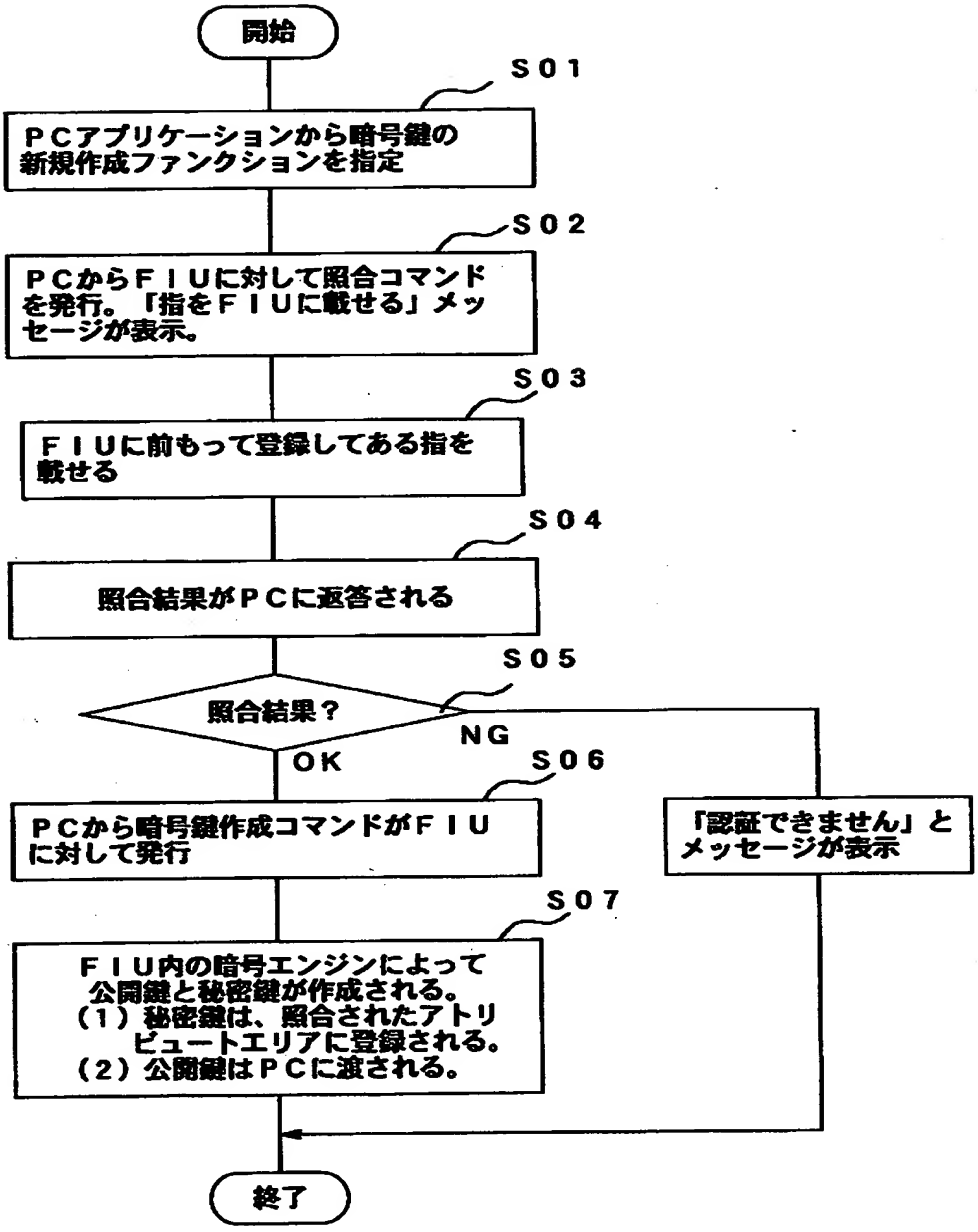
【図１】


１００　指紋照合装置
１１２
CCD
レンズ鏡筒
A／D
変換
LED
１１１
１１３
１１４
照合コントローラ
１３０
１４０
RAM
フラッシュ
メモリ
１２０
１８０
RS232C
ドライバ
CPU
プログラム用
RAM
プログラム用
Flashメモリ
暗号エンジン
１６０
１５０
１７０
１９０
３００　通信ケーブル
２００　ホストコンピュータ

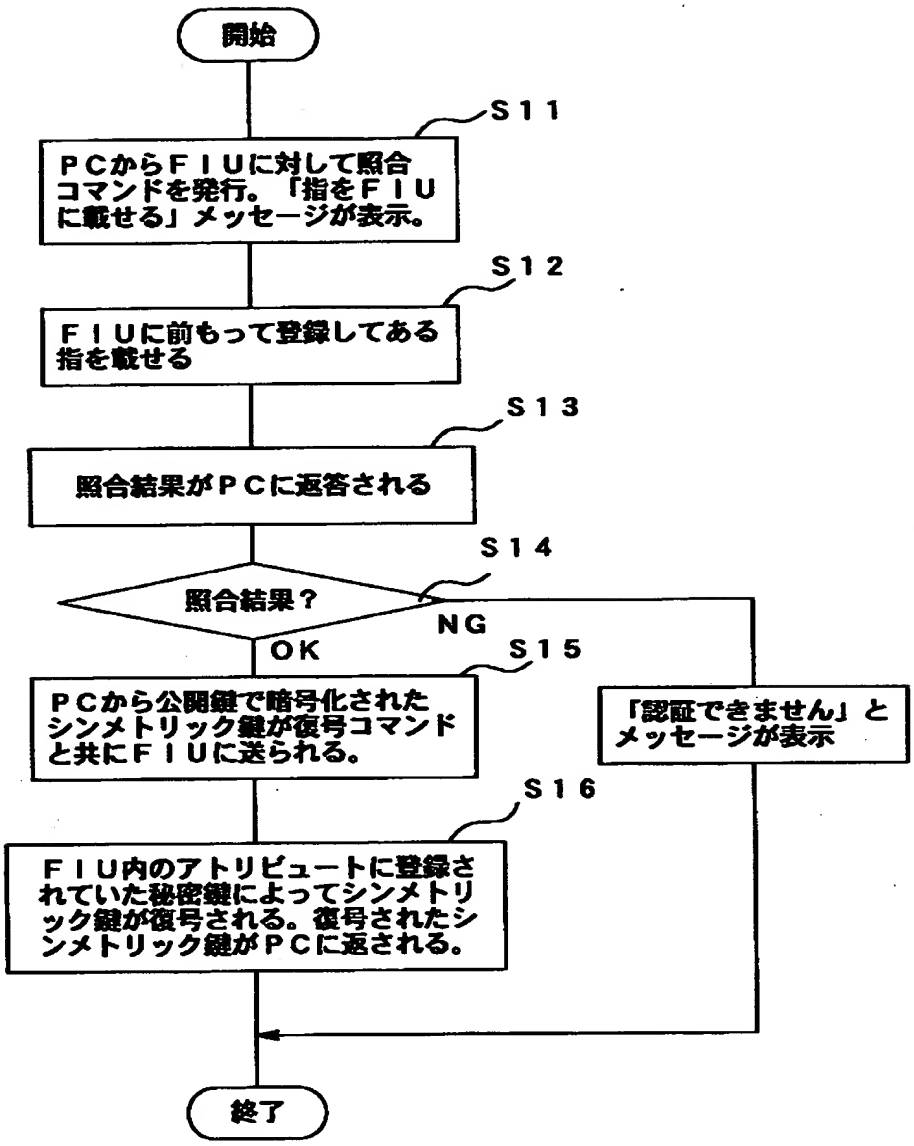
【図２】


インデックス＃１
(512Byte)
インデックス＃２
(512Byte)
インデックス＃９９９
(512Byte)
インデックス＃１０００
(512Byte)
指紋
テンプレート
(256Byte)
アトリビュート
(256Byte)

【図３】


開始
S01
ＰＣアプリケーションから暗号鍵の新規作成ファンクションを指定
S02
ＰＣからＦＩＵに対して照合コマンドを発行。「指をＦＩＵに載せる」メッセージが表示。
S03
ＦＩＵに前もって登録してある指を載せる
S04
照合結果がＰＣに返答される
S05
照合結果？
NG
OK
S06
ＰＣから暗号鍵作成コマンドがＦＩＵに対して発行
「認証できません」とメッセージが表示
S07
ＦＩＵ内の暗号エンジンによって公開鍵と秘密鍵が作成される。
（１）秘密鍵は、照合されたアトリビュートエリアに登録される。
（２）公開鍵はＰＣに渡される。
終了

【図４】


開始
S11
ＰＣからＦＩＵに対して照合コマンドを発行。「指をＦＩＵに載せる」メッセージが表示。
S12
ＦＩＵに前もって登録してある指を載せる
S13
照合結果がＰＣに返答される
S14
照合結果？
NG
OK
S15
ＰＣから公開鍵で暗号化されたシンメトリック鍵が復号コマンドと共にＦＩＵに送られる。
「認証できません」とメッセージが表示
S16
ＦＩＵ内のアトリビュートに登録されていた秘密鍵によってシンメトリック鍵が復号される。復号されたシンメトリック鍵がＰＣに返される。
終了

【書類名】　　要約書

【要約】

【課題】　公開鍵暗号法に用いられる秘密鍵等の重要なデータを安全に保管する。

【解決手段】　使用者が指紋照合装置１００に保管されている保管情報をアクセスする指示をホストコンピュータ２００に入力すると、指紋照合装置１００へ照合指示コマンドが送られる。使用者の指紋をＬＥＤ１１１、レンズ鏡筒１１２、ＣＣＤ１１３、Ａ／Ｄ変換１１４から成る指紋検出手段で読み取り、照合コントローラ１２０により指紋の照合を行い、照合結果が一致していた場合のみ保管情報へのアクセスを許可する。同時に、照合結果はホストコンピュータ１００へ送られる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社